PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-044632
(43)Date of publication of application : 16.02.1996

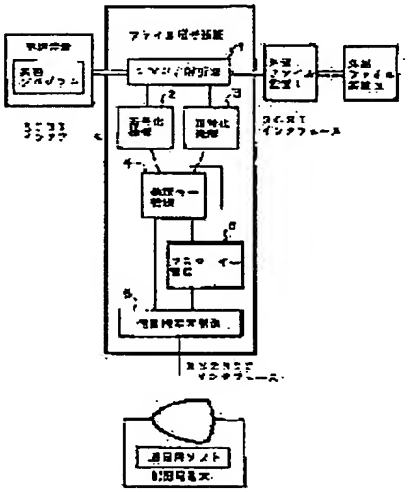
(51)Int.Cl. G06F 12/14
G06F 12/00

(21)Application number : 08-176813
(22)Date of filing : 28.07.1994

(71)Applicant : NEC CORP
(72)Inventor : UMEDA MASAO

(54) FILE CIPHERING DEVICE

(57)Abstract:
PURPOSE: To cipher and decipher a file by using an existent job program or a utility program as it is without correcting it.
CONSTITUTION: This device is provided with a command interpreting part 1 for interpreting an SCSI command, ciphering mechanism 2 for ciphering write data similarly extracted from an external filing device number extracted by the command interpreting part 1, deciphering mechanism 3 for deciphering read data similarly extracted from the external filing device number extracted by the command interpreting part 1, device key management 4 for managing a device key for each external filing device, master key management 5 for managing the master key of the entire file ciphering device, and terminal control 6 for controlling a terminal for control to control the file ciphering device, and this device is connected to an SCSI interface part between a processor and the external filing device.



LEGAL STATUS

[Date of request for examination]	28.07.1994
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	2600643
[Date of registration]	29.01.1997
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号

特開平8－44632

(43)公開日　平成8年(1996)2月16日

(51)Int.Cl.⁶		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ	12/14	３２０　Ｂ			
	12/00	５３７　Ｈ	7623－5Ｂ		

審査請求 有　請求項の数3　ＯＬ　（全４頁）

(21)出願番号　特願平6－176813

(22)出願日　平成6年(1994)7月28日

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目7番1号

(72)発明者　梅田　政夫
東京都港区芝五丁目7番1号　日本電気株式会社内

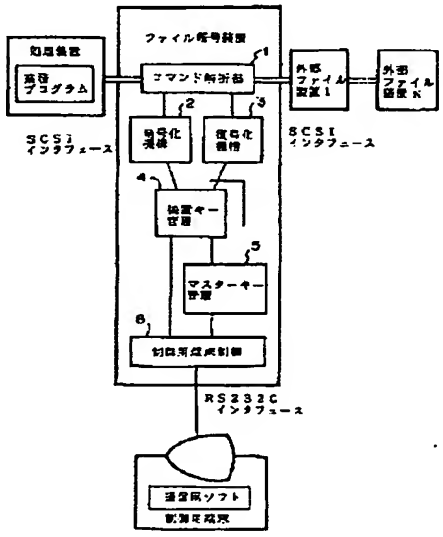
(74)代理人　弁理士　山下　穣平

(54)【発明の名称】　ファイル暗号装置

(57)【要約】

【目的】　既存の業務プログラムもしくはユーティリティプログラムを修正することなくそのまま使用してファイルの暗号化／復号化を可能とする。

【構成】　ＳＣＳＩコマンドを解析するコマンド解析部１と、前記コマンド解析部で抽出された外部ファイル装置番号から同じく抽出された書込みデータを暗号化する暗号化機構２と、前記コマンド解析部で抽出された外部ファイル装置番号から同じく抽出された読込みデータを復号化する復号化機構３と、外部ファイル装置毎の装置キーを管理する装置キー管理４と、ファイル暗号装置全体のマスタキーを管理するマスタキー管理５と、ファイル暗号装置を制御する制御用端末を制御する制御用端末制御６と、を備え、処理装置と外部ファイル装置との間のＳＣＳＩインタフェース部に接続されることを特徴とするファイル暗号装置。



1

【特許請求の範囲】

【請求項1】 ＳＣＳＩコマンドを解析するコマンド解析部と、

前記コマンド解析部で抽出された外部ファイル装置番号から同じく抽出された書込みデータを暗号化する暗号化機構と、

前記コマンド解析部で抽出された外部ファイル装置番号から同じく抽出された読込みデータを復号化する復号化機構と、

外部ファイル装置毎の装置キーを管理する装置キー管理と、

ファイル暗号装置全体のマスターキーを管理するマスターキー管理と、

ファイル暗号装置を制御する制御用端末を制御する制御用端末制御と、を備え、処理装置と外部ファイル装置との間のＳＣＳＩインタフェース部に接続されることを特徴とするファイル暗号装置。

【請求項2】 前記マスターキーは、前記ＳＣＳＩインタフェースに接続される装置すべてに共通であることを特徴とする請求項1に記載のファイル暗号装置。

【請求項3】 装置選択情報として装置毎に暗号の可否を指定する手段を有することを特徴とする請求項1に記載のファイル暗号装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明はファイル暗号装置に関し、特にＳＣＳＩインタフェースで接続される外部ファイル装置内のデータ暗号に関する。

【０００２】

【従来の技術】従来のファイル暗号方式は、図３に示すように外部接続された暗号／復号化装置に対し業務プログラムもしくはファイル入出力制御よりデータを引渡し、ファイル内データの暗号／復号化を行っていた。

【０００３】また、キーの管理については独立したキー管理部を持ち業務プログラムからキーの登録、修正、削除をプログラムから行っていた。

【０００４】従来技術では、業務プログラムの開発時当初からファイル暗号を行う場合は特に問題はなかったが、後からファイル暗号機能を業務プログラムに追加しようとする場合は業務プログラムの変更が必要であった。

【０００５】特開昭５６－４７８５０号公報には、「データ処理方式」として、計算機システム間でのデータの受渡しにおいて、各計算機センタの固有情報と付随情報から秘密データ中の位置を算出し、その位置に暗号を施すことにより、各計算センタでの秘密データの送受を実現する方式が記載されている。

【０００６】

【発明が解決しようとする課題】このような従来のファイル暗号では、業務プログラムに最初からファイル暗号

2

を組込んで開発する場合はよかったが、既にある業務プログラムにファイル暗号を追加する場合は業務プログラムの修正が必要であり、特に業務プログラムがサードパーティの市販プログラムの場合は修正が不可能であり事実上ファイル暗号機能を付加することができないという問題があった。

【０００７】【発明の目的】本発明の目的は、既にある業務プログラムに、その業務プログラムの修正なしに、ファイル暗号機能を付加できるようにすることにある。

【０００８】

【課題を解決するための手段】本発明は、前記課題を解決するため、ファイル暗号装置として、処理装置と外部ファイル装置との間のＳＣＳＩインタフェース部に接続される。ファイル暗号装置はＳＣＳＩを通過するコマンドのうち暗号化／復号化を必要とするコマンドを解析するコマンド解析部、ＳＣＳＩコマンド上のデータを暗号化する暗号化機構、ＳＣＳＩコマンド上のデータを復号化する復号化機構、暗号化機構／復号化機構に外部ファイル装置毎のキーを管理する装置キー管理、個々の装置キー全体の暗号／復号を行うマスターキー管理、外部からキーの入力、修正等を行う為の制御用端末を制御する制御用端末制御を備えている。

【０００９】

【作用】本発明によれば、ファイル暗号／復号化機能を独立した装置として、これを処理装置とフロッピーディスク装置やＣＧＭＴ装置等外部ファイル装置との間に挿入することにより、元の業務プログラムに全く修正をほどこすことなくファイル暗号化及び復号化機能を実現することができるものである。

【００１０】

【実施例】図２は、本発明のファイル暗号装置の接続形態と、データの流れの概略を示す図である。

【００１１】図２において、入出力はＳＣＳＩとし、ＰＣ／ＷＣ側からのデータの内、書込みデータの情報部分のみを暗号化する。又、逆方向のデータについて同様に復号化する。

【００１２】装置に対しては外部より以下の情報の設定、変更、削除等を行う。

（１）マスターキー：ＳＣＳＩインタフェースに接続される装置すべてに共通であり、装置毎の暗号化キーの暗号化用キーである。

（２）装置キー：ＳＣＳＩインタフェースに接続される装置毎に与えられるキーである。

（３）装置選択情報：装置毎に暗号の可否を指定することができる。

【００１３】尚、各情報の設定はＲＳ２３２Ｃを通したＰＣ等で設定／変更することができる。

【００１４】また、暗号方式には特に規定しないが、慣用暗号系のほか、公開鍵暗号方式を使用する場合は、キー情報に公開鍵及び復号用秘密鍵を設定する。

【００１５】図１は、本発明の一実施例のファイル暗号装置の概略構成図である。

【００１６】図１において、コマンド解析部１は、処理装置と外部ファイル装置のＳＣＳＩインタフェース上を流れるコマンド群を解析し制御用コマンド以外のデータ読込み、データ書込み用コマンドを抽出する。データ書込み用コマンドがあった場合は、そのコマンドに付随する書込みデータを暗号化機構２に送り、データ読込み用コマンドがあった場合は、そのコマンドに付随する読込みデータを復号化機構３に送る。この時コマンド解析部はデータに外部ファイル装置番号をコマンド中から抽出しデータに付加しておく。

【００１７】暗号化機構２は、コマンド解析部から送られた外部ファイル装置番号より装置キー管理４を通し暗号化用の装置キーを取得し、これを用いてデータの暗号化を行う。

【００１８】復号化機構３は、コマンド解析部から送られた外部ファイル装置番号より装置キー管理４を通し復号化用の装置キーを取得し、これを用いてデータの復号化を行う。

【００１９】装置キー管理４は、ＳＣＳＩインタフェースに接続される外部ファイル装置毎の暗号／復号化キーを保持する。

【００２０】各装置キーは、このファイル暗号化装置全体で一つのマスターキーで暗号化される。この為、複数のファイル暗号装置間で同一の装置キーであってもマスターキーが異なれば同一に付与された装置キーでも異なったキーとなる。

【００２１】マスターキー管理５は、ファイル暗号装置固有のマスターキーを保持する。

【００２２】マスターキーや装置キーは、ファイル暗号装置にＲＳ２３２Ｃインタフェースで接続されたパソコン等の制御用端末から登録／変更／削除／参照が可能であるが、この制御用端末を制御するのが制御用端末制御６である。

【００２３】尚、制御用端末から操作を行う場合、パスワードにより操作のセキュリティを確保する。

【００２４】

【発明の効果】以上説明したように本発明は、既存の業務プログラムに全く手を入れることなくＳＣＳＩインタフェースに接続された外部ファイル装置内のファイルデータを暗号化することができる。

【００２５】これにより、たとえば外部ファイル装置がリムーバブルな媒体でこれにより実際の媒体を運ぶことによりデータを転送する場合のデータ漏洩の防止が、通常プログラムの修正がむずかしい市販の業務プログラムやユーティリティプログラムを使用した場合でも可能となる。

【００２６】また、従来のシステムに本装置を追加するだけなので、どの様な業種システムでも利用できる。

【００２７】また、装置毎に暗号可否が指定できるので従来と同様のファイル形態も利用できる。

【００２８】また特に、ファイルで外部のシステムと情報交換を行っているシステムには有効である。

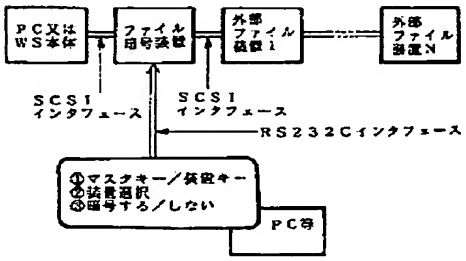
【図面の簡単な説明】

【図１】本発明の一実施例のブロック図である。

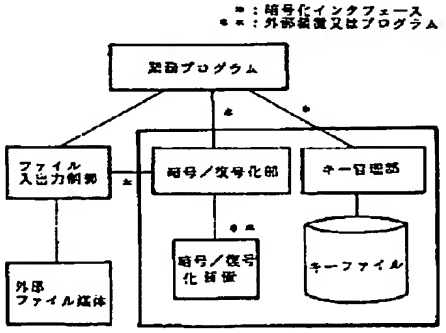
【図２】本発明のファイル暗号装置の接続形態を示すブロック図である。

【図３】従来のファイル暗号／復号化例のブロック図である。

【図２】



【図３】



【図1】